Using a PGP-compatible cryptosystem, I have created a "DH/DSS" private key ("the Private Key") and public key ("the Public Key"). The Public Key uniquely corresponds to a 160-bit "fingerprint" (SHA-1 hash). The fingerprint is printed below as ten groups of four hexadecimal digits, and in various outline fonts throughout the background of this entire paper and in all its signature fields: **FC1D 9CBF B80D E940 6250 7CAD 070F 90BA CDA2 44D0**

The Private Key uniquely corresponds to the Public Key but is computationally infeasible to derive from the Public Key. (Two data sets are said to "uniquely correspond" when it is computationally infeasible that data sets other than those uniquely corresponding could be found to match, using the cryptographic process that is intended to match the data sets.) From time to time, I expect to apply my digital signature to electronic records, with the same legal effect as my ink signature would have on a printed copy thereof. When I do so, a set of signature data is produced that uniquely corresponds to both the document being signed and the Public Key. The slightest change in a document so signed will cause the digital signature to no longer match it.

By executing this authentication and certification instrument ("ACI"), I acknowledge, stipulate, and covenant that any electronic record accompanied by a digital signature that uniquely corresponds to both the document and the Public Key (in accordance with the Digital Signature Standard) was signed by me, beyond any reasonable level of doubt. I COVENANT WITH ANY BEARER OF THIS AUTHORIZATION OR FACSIMILE COPY THEREOF NOT TO REPUDIATE SUCH DIGITAL SIGNATURE UNLESS I COMMUNICATE A REVOCATION OF THE PUBLIC KEY TO THE BEARER IN WRITING BEFORE THE SIGNATURE DATE. (A "writing" is an electronic record signed with the digital signature or a paper signed with my ink signature.) A revocation will be deemed constructively communicated upon publication at **SelfCertify.com**.

I agree to always keep the Private Key encrypted (except during brief intervals of use) with a secure passphrase that only I know, to never reveal the passphrase to **anyone** (except as compelled to do so by law), and to use the Private Key only on trustworthy computer systems. I understand that the consequence of failing to do so is the possible forging of my digital signature, which is subject to the non-repudiation covenant above. I understand that to be trustworthy, a computer system must employ computer hardware, software, and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonably reliable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security principles. (Digital Signature Guidelines, American Bar Association, 1996.) I have read, understand, and agree to follow guidelines provided to me by **SelfCertify.com** for selecting a secure passphrase and for ensuring that all computer systems on which I use the Passphrase remain trustworthy.

Any ACI (or facsimile copy thereof) including (1) language substantially identical to that above, (2) the fingerprint (or key value) of any other public key, and (3) what is purported to be my notarized handwritten signature is presumed to be a forgery **unless** it is accompanied by a written revocation of the Public Key of this ACI or a digitally signed ACI of the other key, signed with the Public Key of this ACI. The written revocation can be signed with my original, notarized ink signature or digitally with the Public Key of this ACI.

Signed at _____, _____ this _____ day of _____, _____   By: _____

    City   *State*   *Date*   Thomas E. Workman, Jr.

This _____ day of _____, the above-named person personally came before me, produced a mailing label of an overnight delivery package listing him or her as the addressee and two forms of identification (including one with a matching photograph). The person then executed the foregoing ACI in my presence. On the line below, I have written the mailing or tracking number of the mailing label. I will mail this signed document directly to **SelfCertify.com** at the return address shown on the mailing label.

Label No. _____

Notary Public: _____

My commission expires: _____

For Certified Copies: This document is certified to be a true copy of the original document signed in ink.

Notary Public: _____
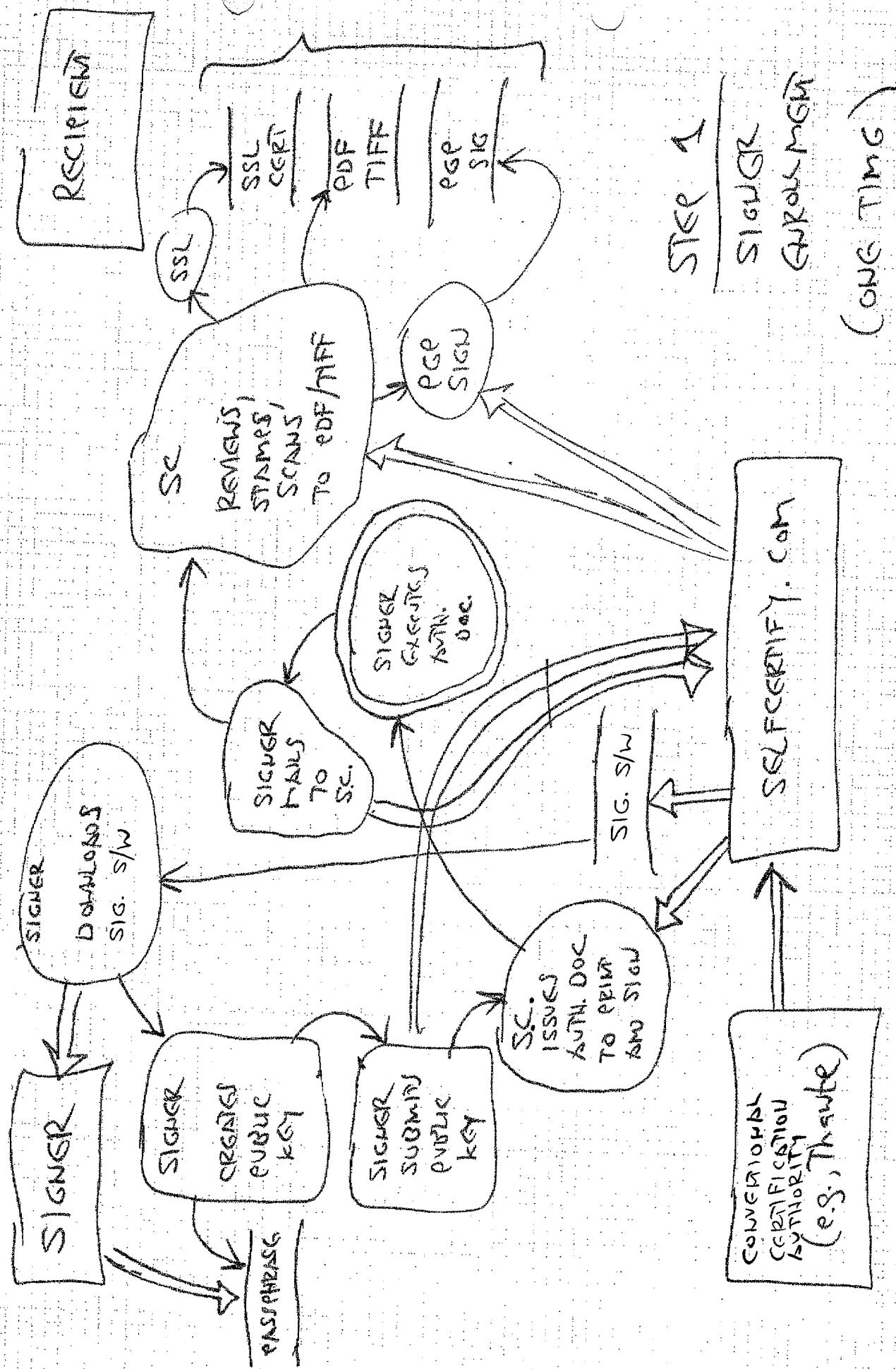

Notary: Outline digits are in background of entire document. Please stamp over digits in space above.

Certifying Notary: Please stamp above with comm. expiry date.
Notary for original document: Please leave blank.

A-1

RECIPIENT

SSL CERT

PDF/TIFF

PGP SIG

SSL

SC REVIEWS, STAMPS, SCANS TO PDF/TIFF

PGP SIGN

STEP 1

SIGNER ENROLLMENT (ONE TIME)

SIGNER CHECKS AUTH. DOC.

SIGNER FAILS TO S.V.

SELFCERTIFY.COM

SIGNER DOWNLOADS SIG. S/W

SIG. S/W

SC. ISSUES AUTH. DOC. TO PRINT AND SIGN

SIGNER

SIGNER CREATES PUBLIC KEY

SIGNER SUBMITS PUBLIC KEY

CONVENTIONAL CERTIFICATION AUTHORITY (e.g., THAWTE)

PASSPHRASE

B-1

RECIPIENT

RECIPIENT FOLLOWS INSTRUCTIONS
#1 - DOWNLOAD REGULAR W/ LATEST SIGNED PUBLIC KEY FILE

INST. #2
DOWNLOAD PUBL. DOC. FOR SIGNER

INST. #3
VERIFY MESSAGE

SIGNED MESSAGE W/ INSTRUCTIONS

NOTE ↑

SELFCCERTIFY1.com

STEP 2

SIGN + VERIFY

SIGNER SIGNS MESSAGE

SIGNER SIGNS INSTRUCTIONS

SIGNER

PASSPHRASE

MESSAGE

INSTRUCTIONS

NOTE 1:
#2 DEPLOYA — BECAUSE KEYFILE SIGNED BY SELFCERTIFY.com (W/ PROMPT?) OR JUST SSL?

B-2